De privacy van de (smart) citizen in de smart city

door Natascha van Duuren

Smart cities roepen complexe juridische vragen op. Veel van deze vraagstukken zijn gerelateerd aan data. Smart cities verzamelen immers data of combineren data op diverse manieren. Soms worden ook risicoprofielen gemaakt of zelfs besluiten genomen. In deze bijdrage wordt op een aantal van deze vragen ingegaan en wordt getracht een oplossingsrichting te geven.

Smart city en de Nederlandse strategie

De term 'smart city' bestaat sinds 2005 en is geïntroduceerd door grote techbedrijven als IBM, Siemens en Cisco. In 2017 werd het onderwerp op de agenda van onze overheid gezet en werd de NL Smart City Strategie gepresenteerd: 'The future of living'.

De voordelen van smart cities zijn helder. Zij kunnen bijdragen aan het oplossen van grote maatschappelijke problemen, zoals klimaat en energiegebruik. Daarnaast zijn er ook oplossingen waarvan de voordelen voor de meeste mensen wat concreter zijn. Denk aan slimme camera's die lege plekken tellen in fietsenstallingen. Maar ook aan lantaarnpalen die geluid en luchtkwaliteit meten of de omgeving filmen, slimme sensoren

in afvalbakken en stoplichten die vaker groen geven voor fietsers als het regent. Een heel actueel voorbeeld is natuurlijk crowdmanagement, ingezet tijdens de coronapandemie.

Data, veel data

In smart city-projecten worden veel data verzameld, waaronder persoonsgegevens. Op grond van art. 15 AVG moeten burgers niet alleen vooraf worden geïnformeerd, maar ze moeten ook inzage kunnen krijgen in de dataverzameling. In de praktijk lijkt het lastig om aan deze eisen te voldoen. In een smart city worden burgers niet of nauwelijks geïnformeerd welke persoonsgegevens worden verzameld en voor welk doel. De vraag is hoe deze informatieplicht concreet kan worden ingericht? De hele stad volhangen met teksten waarmee de burger wordt ingelicht? Of een systeem met iconen die de burger informeren?

Een bijkomende complexiteit is dat gemeenten soms zelf nauwelijks een overzicht hebben van alle persoonsgegevens die in hun smart city worden verwerkt. De smart city lijkt in dat geval een black box voor de gemeente, wat het zeer lastig maakt aan de informatieplicht te voldoen.

Anonieme persoonsgegevens?

Veel gemeenten geven aan dat zij in hun smart cities alleen gebruikmaken van 'anonieme gegevens'. In veel gevallen bedoelen ze daarmee dat zij gebruikmaken van gepseudonimiseerde gegevens. Pseudonimiseren is een beveiligingsmaatregel waarbij persoonsgegevens worden verwerkt zonder dat daarbij duidelijk wordt over welke personen die gegevens gaan. Gegevens kunnen alleen nog herleidbaar zijn tot een specifiek persoon als er gebruik wordt gemaakt van aanvullende gegevens. Bij pseudonimisering gaat het echter nog steeds om persoonsgegevens. De gemeente is dus nog steeds verplicht te voldoen aan de privacywet en -regelgeving.

Ook al zou het zo zijn dat een gemeente uitsluitend anonieme gegevens verwerkt, ook dan moeten gemeenten zich realiseren dat geanonimiseerde gegevens makkelijker op personen zijn terug te voeren dan men veelal

denkt. Onderzoekers van de Amerikaanse MIT-universiteit kwamen tot de conclusie dat je maar vier informatiepunten nodig hebt, zoals locaties of aankopen, om 90 procent van de individuen te kunnen identificeren.

Met het argument van gemeenten dat zij in smart cities 'alleen maar anonieme gegevens verwerken', zijn ze er dus niet. Gemeenten doen er in hun risicoanalyse goed aan, ervan uit te gaan dat zij met persoonsgegevens te maken hebben (en dat zij derhalve aan de wet- en regelgeving voor privacy moeten voldoen).

Risico van structurele benadeling van bepaalde groepen, onterechte uitsluiting of stigmatisering van burgers in de smart city

In smart cities worden niet alleen veel data verzameld, maar deze data worden ook met elkaar gecombineerd. Denk aan het combineren van verzuimcijfers met data over werkloosheid, schulden, overgewicht, politiecijfers en social-mediaberichten. Aan de hand hiervan kan bijvoorbeeld worden getracht het risico van schooluitval te voorspellen. Een nog verdergaande stap is dat op basis van data besluiten worden genomen. De AVG stelt strenge eisen aan dit soort gegevensverwerkingen.

Zo zal de gemeente burgers moeten informeren over de 'onderliggende logica' van het algoritme. Op begrijpelijke wijze moet duidelijk worden gemaakt op basis van welke criteria tot een besluit wordt gekomen.

Verder kent de AVG als uitgangspunt dat niemand onderworpen mag worden aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit waaraan voor hem of haar belangrijke (rechts)gevolgen zijn verbonden (art. 22 AVG). In dat geval moet de burger altijd de mogelijkheid hebben om een mens (alsnog) naar het besluit te laten kijken, zijn of haar standpunt kenbaar te maken of het besluit in rechte aan te vechten. Vergelijkbare waarborgen vloeien voort uit de Algemene wet bestuursrecht (Awb), voor zover het besluit zou gelden als een besluit van een bestuursorgaan.

Uiteraard dient voorkomen te worden dat algoritmes vooroordelen hebben. Een smart city mag niet leiden tot het structureel benadelen van bepaalde groepen, tot onterechte uitsluiting of stigmatisering. Vaak realiseert men zich niet dat dit al begint bij de dataverzameling: welke data verzamel je en welke categorieën (bijvoorbeeld groepen) onderscheid je daarbij? Een terechte zorg die wel eens wordt genoemd in het kader van een smart city is dat een smart city *social chilling* of *social cooling* zou kunnen veroorzaken. Hiermee bedoelt men dat mensen zich conformeren aan de geldende normen en zich gereserveerd gedragen, niet-creatief en risicomijdend. De ethische vraag die daarmee samenhangt – en die ook terecht wordt gesteld – is in hoeverre burgers imperfect mogen zijn en mogen afwijken van de gedefinieerde normen? Normen die in feite door data gedefinieerd zijn. Bovendien moeten bestuurders van slimme steden zich goed realiseren dat een patroon in data niet de werkelijkheid hoeft te zijn. Met andere algoritmes zou je immers andere uitkomsten kunnen krijgen. In slimme steden moeten de uitkomsten van algoritmes en data-analyses dan ook steeds getoetst worden.

Cyber security moet in een smart city prioriteit nummer één zijn

De grote hoeveelheid data die in een smart city wordt verwerkt, betekent dat informatiebeveiliging prioriteit nummer één moet zijn. Stel je eens een cybercrime aanval op een smart city voor. Er bestaat niet alleen het risico dat (gevoelige) gegevens van vele burgers op straat komen te liggen. Het kan ook zijn dat de cyberaanval gericht is op nutsvoorzieningen of andere voorzieningen uit de vitale sector. Dit met alle gevolgen van dien. In een smart city moet informatiebeveiliging dan ook boven aan de beleids- en uitvoeringsagenda staan. Het is de vraag of de Baseline Informatiebeveiliging Gemeenten (BIG) afdoende is om smart cities tegen dit soort risico's te beveiligen. Dit is dan ook de reden dat gemeenten aan het begin van ieder smart city-project een Data Protection Impact Assessment (DPIA) moeten organiseren, die de grootste risico's zou moeten kunnen identificeren.

Risico van te grote afhankelijkheid van machtige technologiebedrijven

Zoals eerder opgemerkt is de smart city destijds geïntroduceerd door grote techbedrijven. Ook nu spelen grote techbedrijven vaak een belangrijke rol in smart cities. Het lijkt immers bijna onmogelijk een smart city te bouwen zonder gebruik te maken van cloud- en platformoplossingen. Naast het feit dat dit vaak grote en machtige partijen zijn, komen deze partijen meestal uit de VS. Onze digitale infrastructuur is voor een groot deel afhankelijk van de VS en van China. Dit is zeker een punt van aandacht. Gemeenten doen er goed aan kritisch te zijn op de private partijen die zij inschakelen en welke afspraken er met deze partijen kunnen worden gemaakt. Daarbij dienen gemeenten zich te realiseren dat het businessmodel van bedrijven die zich in de smart city-markt begeven, soms volledig is gebaseerd op het 'nieuwe goud': data. Zij zullen er dan ook alles aan doen om deze data niet openbaar te maken. Dit staat uiteraard op gespannen voet met de (privacy)wetgeving. Ook het risico van vendor lock-in ligt op de loer. Met andere woorden, door contractafspraken en vergaande verwevenheid van procesafspraken kunnen gemeenten geen andere leveranciers meer contracteren. Het is dus van groot belang dat gemeenten voorkomen dat zij bij de realisatie van een smart city afhankelijk worden van grote machtige technologiebedrijven.

The future of living?

Het Rathenau Instituut heeft zeven publieke waarden geïdentificeerd die in de slimme stad onder druk kunnen komen te staan: privacy, veiligheid, rechtvaardigheid, autonomie, controle over technologie, menselijke waardigheid en machtsevenwicht.

Een aantal van deze publieke waarden is in deze bijdrage besproken. Dat de andere waarden onbesproken zijn gebleven, betekent niet dat deze minder belangrijk zijn. Het borgen van deze waarden in een smart city is complex. Dit is waarschijnlijk ook de reden dat smart cities langzaam van de grond lijken te komen. Een belangrijke stap voorwaarts is dat VNG-leden hebben ingestemd met de Principes Digitale Samenleving.

Dit gemeenschappelijke kader zorgt ervoor dat er in elke gemeente gelijke spelregels gelden voor gesprekken met aanbieders. Dit kan zorgen voor een versterking van de positie van gemeenten in de richting van de (soms machtige) marktpartijen. De principes moeten tegelijkertijd de publieke waarden van de burger borgen, waaronder uiteraard de privacy van de (smart) citizen in de smart city.

- In een smart city worden veel persoonsgegevens verzameld van burgers. Het lijkt niet eenvoudig om in een smart city aan de wettelijke informatieplicht te voldoen. Opties als de hele stad volhangen met teksten waarmee de burger wordt ingelicht of een systeem met iconen die de burger informeren, stuiten al snel op praktische bezwaren. Ook het feit dat de smart city vaak een black box is voor gemeenten, maakt het voldoen aan de wettelijke informatieplicht niet eenvoudig.
- Gemeenten dienen zeer alert te zijn op het risico van structurele benadeling van bepaalde groepen, onterechte uitsluiting of stigmatisering van burgers. Deze risico's kunnen in een smart city op de loer liggen.
- Het lijkt bijna onmogelijk een smart city te bouwen zonder gebruik te maken van cloud- en platformoplossingen. Gemeenten dienen daarbij te voorkomen dat zij afhankelijk worden van machtige (vaak buitenlandse) technologiebedrijven.

Bronnen

- Autoriteit Persoongegevens. (2019, 7 oktober). Waarborg privacy in de ontwikkeling van Smart Cities. Geraadpleegd op https://autoriteitpersoonsgegevens.nl/nl/nieuws/waarborg-privacy-de-ontwikkeling-van-smart-cities.
- Future City Foundation. (2019, oktober). Een slimme stad zo doe je dat. Geraadpleegd op https://future-city.nl/bestel-het-boek-een-slimme-stad-zo-doe-je-dat/.
- The Hague Security. (2017, januari). Delta. NL Smart City Strategy. Geraadpleegd op https://www.thehaguesecuritydelta.com/media/com_hsd/report/114/document/NL-Smart-City-Strategie-.pdf.
- Informatiebeveiligingsdienst. (2016, juni). Tactische baseline informatiebeveiliging Nederlandse gemeenten. Geraadpleegd op https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2016/07/Tactische-Baseline-Informatiebeveiliging-Nederlandse-Gemeenten-v1.02.pdf.
- Mulder, E. (2017, november). Smart Cities: een internationaal perspectief. Geraadpleegd op https://www.forumstandaardisatie.nl/sites/default/files/BFS/4-basisinformatie/publicaties/Smart-Cities-een-internationaal-perspectief.pdf.
- Naafs, S. (2017, 6 december). De muren hebben sensoren. Geraadpleegd op https://www.groene.nl/artikel/de-muren-hebben-sensoren.
- Raaphorst, R. (2018, 13 november). Zeven waarden onder druk. Geraadpleegd op https://future-city.nl/zeven-waarden-onder-druk.
- Rathenau Instituut. (2017, 17 november). De slimme stad in de praktijk. Geraadpleegd op https://www.rathenau.nl/nl/digitale-samenleving/de-slimme-stad-de-praktijk.
- Rathenau Instituut. (2017, 30 november). Hoe beschermen gemeenten publieke waarden in de slimme stad? Geraadpleegd op https://www.rathenau.nl/nl/digitale-samenleving/hoe-beschermen-gemeenten-publieke-waarden-de-slimme-stad.
- Rathenau Instituut. (2017, 17 november). Steden gedreven door data. Geraadpleegd op https://www.rathenau.nl/nl/digitale-samenleving/steden-gedreven-door-data.
- Uitvoeringswet Algemene verordening gegevensbescherming (2020, 1 januari). Geraadpleegd op https://wetten.overheid.nl/BWBR0040940.
- VNG. (2019, 1 november). Principes voor de digitale samenleving. Geraadpleegd op https://vng.nl/sites/default/files/2019-11/lbr-19-091.pdf.
- VNG. (2019, 29 november). VNG leden akkoord met principes digitale samenleving. Geraadpleegd op https://vng.nl/nieuws/vng-leden-akkoord-met-principes-digitale-samenleving.